

Information Security Management System (ISMS)

Alexander Gesinn

Emotet, Phishing, Social Engineering...



... digital transformation, cloud services, home office

PRODUCTIVITY



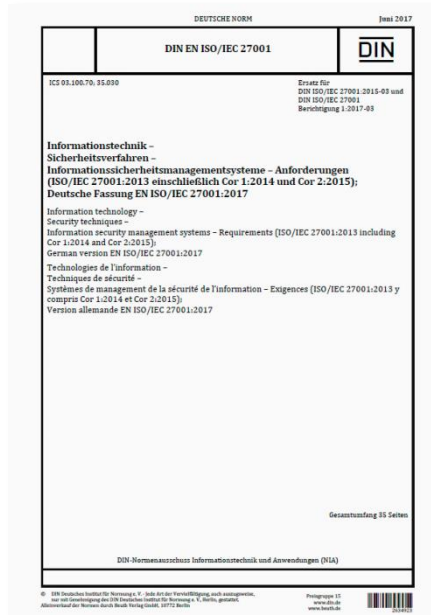
IT security is important, but where and how to start?

Information Security Management System (ISMS)

- describes controls
- that an organization needs to implement
- to ensure that it is sensibly protecting
- the confidentiality, availability, and integrity of assets
- from threats and vulnerabilities.

ISMS Best Practices

ISO/IEC 27001

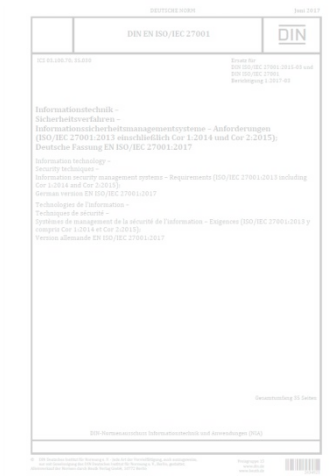


IT-Grundschutz BSI 200-x



ISMS Best Practices

ISO/IEC 27001



IT-Grundschutz BSI 200-x



IT-Grundschutz BSI 200-x

- **reduce the expenses of the information security process.**
- **known approaches and methods for improvement of information security are combined and updated continuously.**
- **IT-Grundschutz Compendium: methods with concrete security safeguards for typical business processes, applications, systems, communication links and rooms**

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html

IT-Grundschutz Compendium



IT-Grundschutz-Standards

Die BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen, Vorgehensweisen und Maßnahmen zur Informationssicherheit.



IT-Grundschutz-Kompendium

IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium ist die modernisierte Fassung der IT-Grundschutz-Kataloge.



IT-Grundschutz-Profile

Schablonen, mit denen verschiedene Anwender(-gruppen) selbstständig den IT-Grundschutz auf ihre Bedürfnisse anpassen können.

<https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html>

Process-oriented modules:

- **ISMS (Information Security Management Systems)**
- **ORP (Organisation and Personnel)**
- **CON (Concepts)**
- **OPS (Operation)**
- **DER (Detection and Reaction)**

• System-oriented modules:

- **INF (Infrastructure)**
- **NET (Networks and Communication)**
- **SYS (IT Systems)**
- **APP (Applications)**
- **IND (Industrial IT)**



Federal Office
for Information Security



SYS.1.1: General Server

Description

Introduction

This module covers general security requirements for all IT systems which make services available to other IT systems, such as clients or other servers. These services can be basic services for the local or external network, but also those that allow the exchange of e-mails or make databases and printer services available. Servers play a key role in information technology, and thus in the well-functioning workflows of an organisation. Servers often perform tasks without users making direct, interactive use of them. In addition, there are server services which directly interact with users and are not perceived as a server service at first glance – for example, X Server in Unix.

Objective

The objective of this module is to protect information which is processed, offered or transmitted by servers, as well as the associated services.

Not in Scope

IT-Grundschutz Compendium

SYS.1.1:General Server - Requirements

Requirements

The specific requirements of module SYS.1.1 *General Server* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Building Services

Basic Requirements

For module SYS.1.1 *General Server*, the following requirements **MUST** be implemented as a matter of priority:

SYS.1.1.A1 Appropriate Installation [Building Services]

Servers **MUST** be operated at locations that may only be accessed by authorised persons. Servers **MUST** therefore be set up and installed in data centres, computer rooms, or lockable server rooms (see the corresponding modules). It **MUST** be regulated who is granted access to the rooms or physical access to the servers themselves. Servers **MUST NOT** be used as personal computers. It **MUST** be ensured that only dedicated removable storage devices and other devices can be connected to the servers.

IT-Grundschutz Compendium

SYS.1.1:General Server – Cross Referencing Threats

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.1 General Server:

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

Elementary Threats	G 0.8	G 0.9	G 0.14	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.44	G 0.45	G 0.46
Requirements																							
SYS.1.1. A1	X	X		X						X	X										X		
SYS.1.1. A2			X			X		X							X								
SYS.1.1. A3			X			X		X							X		X						X
SYS.1.1.		X				X									X		X						X

gesinn.it GmbH & Co. KG



Am Koweier 8f, 92521 Schwarzenfeld



Franz-Mayer-Straße 1, 93053 Regensburg



+49 9435 65218-0



<http://gesinn.it> <http://semantic.wiki>



@gesinn_it